



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/537,300

06/02/2005

Marc Joye

1032326-302

1466

21839 7590 12/16/2008  
BUCHANAN, INGERSOLL & ROONEY PC  
POST OFFICE BOX 1404  
ALEXANDRIA, VA 22313-1404

EXAMINER

CHAI, LONGBIT

ART UNIT

PAPER NUMBER

2431

NOTIFICATION DATE

DELIVERY MODE

12/16/2008

ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ADIPFDD@bipc.com

### **Advisory**

1. Applicant asserts that Drexler fails to teach “a cryptographic method during which an integer division of the type  $q = a \text{ div } b$  and/or a modular reduction of the type  $r = a \text{ mod } b$  is performed, where  $q$  is a quotient,  $a$  is a number containing  $m$  bits,  $b$  is a number containing  $n$  bits, with  $n$  less than or equal to  $m$  and  $b_{n-1}$  is non-zero,  $b_{n-1}$  being the most significant bit of the number  $b$ ” (Remarks: Page 3 / last Para). Examiner respectfully disagrees because (a) the claim language “ $q = a \text{ div } b$  **and/or** a modular reduction” is considered by Examiner as merely a singular selection of “a modular reduction” as set forth in this prior-art rejection (Drexler: Para [0004], Para [0007] and Para [0020]: a modular reduction used for a encryption / decryption process), which is sufficient to meet the claim language of “and / or”, (b)  $Y = M^d \text{ mod } n$ , as taught by Drexler (Para [0007]), is qualified as a modular reduction with  $Y$  as the result of modular reduction matching the claim language of (a type  $r$ ); besides,  $n$  (as a modulus) is indeed less than or equal to  $M^d$  which provides the calculation process of encryption or data scrambling (Drexler: Para [0004], Para [0012] and Para [0020]) that is also qualified as a cryptographic method, as recited in the claim, and is performed in a semiconductor chip (Drexler: Para [0011]) which contains and manipulates the data in a unit of bits in the semiconductor chip having at least one data with a nonzero MSB-bit).
2. Applicant further asserts that Drexler fails to teach “masking the number  $a$  by a random number  $p$  before performing the integer division and/or the modular reduction” (Remarks: Page 5 / 5<sup>th</sup> Para). Examiner respectfully disagrees because Drexler teaches a random number  $r$  is first chosen for modular process ( $M \text{ mod } n$ ) by forming a product

Art Unit: 2431

of  $(r * n)$  which is added to the message  $M$ , where  $n$  is the modulus, as taught by Drexler – this is also consistent with the disclosure of the specification of the instant application (SPEC: Page 10 Line 5: i.e., for modular process  $(a \bmod b)$  in order to mask the number  $a$ ,  $b$  times the random number  $p$  is added to the number  $a$ , i.e.  $a$  is replaced with  $a + (b * p)$ )).

3. Furthermore, Applicant asserts that Drexler fails to teach “generating encrypted or decrypted data in accordance with the results of the division and/or modular reduction” (Remarks: Page 5 / 3<sup>rd</sup> Para). Examiner respectfully disagrees because Drexler teaches an encryption process with a result using  $(\bmod n)$  modular reduction after completion of exponential process (Drexler: Para [0020] Line 1 – 3 / Line 14 – 16 and Para [0005]). Thereby Drexler does teach “generating encrypted or decrypted data in accordance with the results of the division and/or modular reduction” and as such Applicant's arguments are respectfully traversed.